15 MAY 1981

MEMORANDUM FOR THE RECORD

FROM: [redacted] 25X1
Programs Development Branch, ISSG

25X1 [redacted]
Operations Evaluation Branch, ISSG

SUBJECT: Briefing of two members [redacted] 25X1
[redacted] 25X1

REFERENCE: ODP 81-462, dtd 10 April 1981
ODP 81-566, dtd 1 May 1981

1. On 6 May 1981, from 1315 to 1445 hours, subjects were provided an informal briefing of specific areas of interest in the Information Systems Security area as they relate to the 25X1 current efforts of the [redacted] to develop and implement a large 25X1 computerized system [redacted] In essence, we shared with them some specific security suggestions/recommendations which could be useful in their efforts to develop this new system. Reference (attached) provides background information regarding the system plans, configuration time schedules, etc. Hardware and software vendors were unknown at this time. [redacted] 25X1

2. Attachment II reflects the viewgraphs used in this presentation. We skimmed over the Physical/Personnel security portion of our outline in that we discovered early on that they were more interested in the systems security area than in the physical or procedural areas (although they did take notes in areas of tape/disk control, concerns in maintenance area, output 25X1 controls, etc.). [redacted]

3. Areas of particular interest included desired hardware and software features involving selective access to system(s); logging all attempts to access; memory and magnetic media sanitization user identification, and event log inspection. Also included were security testing and theft and copy protection. We pointed out to them that they were fortunate to be considering these security issues early on in that it is much easier to design-in security features (via statement of work/RFP, etc.) than trying to retrofit after a system is "on the air". [redacted] 25X1

WARNING NOTICE
INTELLIGENCE SOURCES
AND METHODS INVOLVED

[redacted] 25X1

4. We provided our guests with one copy of the Willis Ware Report (reissued 1979-unclassified) published by RAND Corp entitled "Security Controls for Computer Systems" and another paper (FREY-unclassified outlining general security requirements which we would like to see in computer systems processing "multi-level" data). NOTE: At no time did we mention specific "installation unique" information (e.g., system specific password thresholds) which would be particularly sensitive from a counterintelligence standpoint. [redacted] 25X1

5. Our remarks generated lively exchange of ideas in areas mentioned. Our suggestions included:

- separation of I/O from main computer center (to control access)

- Strict tape/disk /(incl floppy) control

- Software terminal disconnect features

- On Line audit (by exception)

- Use of SMF (if IBM system) for auditing

- Memory clear

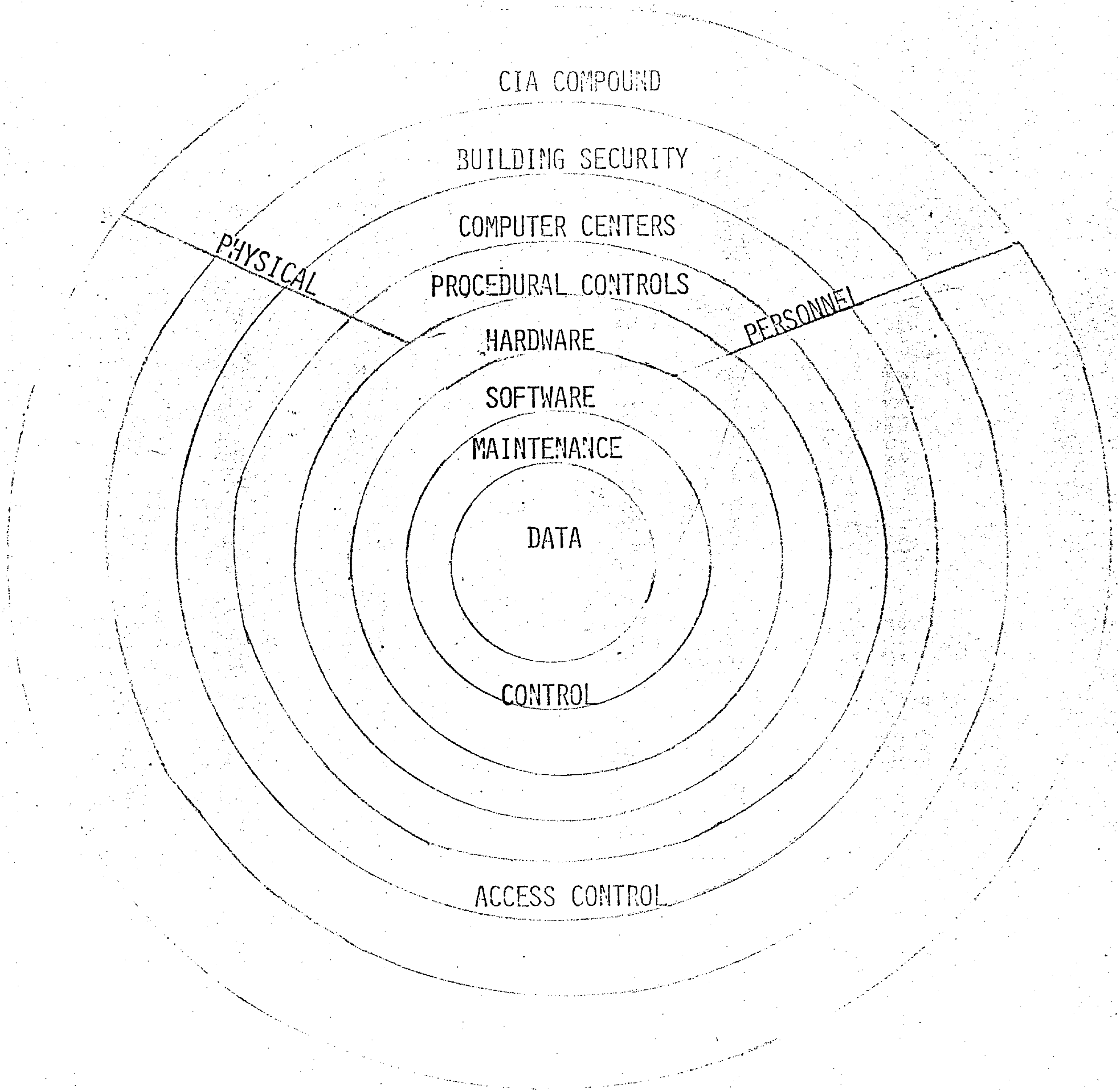
- Restricted Memory dumps

6. At the conclusion they asked for a copy of viewgraphs which have since been provided them. We also volunteered our assistance should they need it and that they could contact us through established channels. The only other person present throughout interview was [redacted] 25X1

[redacted] 25X1

Attachment I - ODP81-462
II - Viewgraphs

"TOTAL" APPROACH TO ADP SECURITY



ADP SYSTEMS SECURITY

I. COMPUTER CENTER ACCESS

PHYSICAL/PERSONNEL SECURITY

- CENTER - OPEN VS. SECURE
- ACCESS CONTROL/BADGE SYSTEM
- CONTROL OF MAINTENANCE PERSONNEL
- TAPE/DISK LIBRARY & CONTROL
- PERSONNEL STAFFING AND CHECKS
- IBM 3350 FIXED DISK PROBLEM

PHYSICAL SWITCH

POWER DOWN

5/5

II. REMOTE TERMINAL OPERATION

- LOCATED IN SECURE/UNSECURED AREAS
- TERMINALS W/BUFFER MEMORY
- SOFTWARE FEATURES TO DISCONNECT
- AUDIT TRAIL FOR USER MANAGEMENT
- TERMINAL - INPUT/OUTPUT

  CLASSIFIED LABLES - I/O
- USERID/PASSWORD PROTECTION MECHANISMS

III. PROCEDURAL

- TAPE I/O CONTROL
- OUTPUT CONTROLS
- FLOPPY DISKS
- DIAGNOSTICS

IV. SYSTEM SECURITY

- MAIN MEMORY OVERWRITE
- AUTOMATIC TERMINAL DISCONNECT
- LOCK OUT TERMINAL FEATURE
- ROLE OF SMF DATA FOR AUDITING
- ACF-2

V. PERSONNEL SECURITY

VI. THREAT

- PROBLEM - CASES - HISTORY
- GOVERNMENT AND INDUSTRY - WHAT DOES EVIDENCE SHOW?

OTHER TOPICS

- CONTRACT EFFORTS.

  TEST METHODOLOGY.

- AUDIT TRAIL EFFORTS.

  CONTRACT TO STUDY HSTS/AUDIT

- AUTHENTICATION DEVELOPMENTS.

  SIGNATURE VERIFICATION

  PALM PRINTS